

-2-

IN THE CLAIMS

Amended claims follow. Insertions are underlined, while deletions are struck out. The status of each claim is included prior to each heading.

1. (Currently Amended) A method of remotely detecting vulnerabilities on a local computer, comprising:
 - a) installing an agent on a local computer;
 - b) receiving encrypted commands for executing a risk-assessment scan from a remote computer utilizing a network;
 - c) decrypting the commands on the local computer utilizing the agent;
 - d) processing the commands on the local computer utilizing the agent; and
 - e) performing the risk-assessment scan on the local computer in accordance with the processed commands to remotely detect local vulnerabilities on the local computer;wherein the agent includes a plurality of risk-assessment modules;
wherein the commands execute the risk-assessment modules in a specific manner that is configured at the remote computer;
wherein the commands each indicate at least one of the risk-assessment modules;
wherein the commands are processed by extracting parameters associated with the commands, and executing the risk-assessment modules indicated by the commands utilizing the associated parameters.
2. (Cancelled)
3. (Cancelled)
4. (Currently Amended) The method as recited in claim 21, wherein the risk-assessment modules are selected for the agent based on specifications of the local computer.

-3-

5. (Currently Amended) The method as recited in claim 21, wherein the risk-assessment modules include a STAT module for performing a stat system call on a file, a READ module for reading a file, a READDIR module for returning contents of a directory, a FIND module for locating a list of files based on a given function, a GETPWENT module for retrieving an entry from a password database, a GETGENT module for retrieving an entry from a group database, a CHKSUM module for performing a checksum operation on a file, and an EXEC module for executing a command.
6. (Currently Amended) The method as recited in claim 21, wherein the risk-assessment modules are selected from the group consisting of a STAT module for performing a stat system call on a file, a READ module for reading a file, a READDIR module for returning contents of a directory, a FIND module for locating a list of files based on a given function, a GETPWENT module for retrieving an entry from a password database, a GETGENT module for retrieving an entry from a group database, a CHKSUM module for performing a checksum operation on a file, and an EXEC module for executing a command.
7. (Cancelled)
8. (Cancelled)
9. (Original) The method as recited in claim 1, and further comprising transmitting results of the risk-assessment scan from the local computer to the remote computer utilizing the network.
10. (Original) The method as recited in claim 9, and further comprising receiving feedback to the results from the remote computer utilizing the network.
11. (Original) The method as recited in claim 1, wherein the commands are decrypted utilizing a shared key.

-4-

12. (Currently Amended) A computer program product embodied on a computer readable medium for remotely detecting vulnerabilities on a local computer, comprising:
- a) computer code for installing an agent on a local computer;
 - b) computer code for receiving encrypted commands for executing a risk-assessment scan from a remote computer utilizing a network;
 - c) computer code for decrypting the commands on the local computer utilizing the agent;
 - d) computer code for processing the commands on the local computer utilizing the agent; and
 - e) computer code for performing the risk-assessment scan on the local computer in accordance with the processed commands to remotely detect local vulnerabilities on the local computer;
- wherein the agent includes a plurality of risk-assessment modules;
wherein the commands execute the risk-assessment modules in a specific manner that is configured at the remote computer;
wherein the commands each indicate at least one of the risk-assessment modules;
wherein the commands are processed by extracting parameters associated with the commands, and executing the risk-assessment modules indicated by the commands utilizing the associated parameters.
13. (Cancelled)
14. (Cancelled)
15. (Currently Amended) The computer program product as recited in claim ~~13~~12, wherein the risk-assessment modules are selected for the agent based on specifications of the local computer.
16. (Currently Amended) The computer program product as recited in claim ~~13~~12, wherein the risk-assessment modules include a STAT module for performing a stat system call on a file, a READ module for reading a file, a

-5-

READDIR module for returning contents of a directory, a FIND module for locating a list of files based on a given function, a GETPWENT module for retrieving an entry from a password database, a GETGREN module for retrieving an entry from a group database, a CHKSUM module for performing a checksum operation on a file, and an EXEC module for executing a command.

17. (Currently Amended) The computer program product as recited in claim ~~13~~12, wherein the risk-assessment modules are selected from the group consisting of a STAT module for performing a stat system call on a file, a READ module for reading a file, a READDIR module for returning contents of a directory, a FIND module for locating a list of files based on a given function, a GETPWENT module for retrieving an entry from a password database, a GETGREN module for retrieving an entry from a group database, a CHKSUM module for performing a checksum operation on a file, and an EXEC module for executing a command.
18. (Cancelled)
19. (Cancelled)
20. (Original) The computer program product as recited in claim 12, and further comprising computer code for transmitting results of the risk-assessment scan from the local computer to the remote computer utilizing the network.
21. (Original) The computer program product as recited in claim 20, and further comprising computer code for receiving feedback to the results from the remote computer utilizing the network.
22. (Original) The computer program product as recited in claim 12, wherein the commands are decrypted utilizing a shared key.

-6-

23. (Currently Amended) A system ~~for~~ remotely detecting vulnerabilities on a local computer, comprising:
- a) an agent installed on a local computer for receiving encrypted commands for executing a risk-assessment scan from a remote computer utilizing a network, decrypting the commands on the local computer, and processing the commands on the local computer; and
 - b) wherein the risk-assessment scan is performed on the local computer in accordance with the processed commands to remotely detect local vulnerabilities on the local computer;
wherein the agent includes a plurality of risk-assessment modules;
wherein the commands execute the risk-assessment modules in a specific manner that is configured at the remote computer;
wherein the commands each indicate at least one of the risk-assessment modules;
wherein the commands are processed by extracting parameters associated with the commands, and executing the risk-assessment modules indicated by the commands utilizing the associated parameters.
24. (Currently Amended) A system ~~for~~ remotely detecting vulnerabilities on a local computer, comprising:
- a) means for installing an agent on a local computer;
 - b) means for receiving encrypted commands for executing a risk-assessment scan from a remote computer utilizing a network;
 - c) means for decrypting the commands on the local computer utilizing the agent;
 - d) means for processing the commands on the local computer utilizing the agent; and
 - e) means for performing the risk-assessment scan on the local computer in accordance with the processed commands to remotely detect local vulnerabilities on the local computer;
wherein the agent includes a plurality of risk-assessment modules;
wherein the commands execute the risk-assessment modules in a specific manner that is configured at the remote computer;

-7-

wherein the commands each indicate at least one of the risk-assessment modules;

wherein the commands are processed by extracting parameters associated with the commands, and executing the risk-assessment modules indicated by the commands utilizing the associated parameters.

25. (Currently Amended) A method of remotely detecting vulnerabilities from a remote computer, comprising:
- a) sending encrypted commands from a remote computer to an agent on a local computer for executing a risk-assessment scan utilizing a network, the commands adapted for being decrypted and processed on the local computer utilizing the agent for performing the risk-assessment scan on the local computer in accordance with the processed commands to remotely detect local vulnerabilities on the local computer;
 - b) receiving results of the risk-assessment scan from the local computer utilizing the network; and
 - c) transmitting feedback to the results from the remote computer to the local computer utilizing the network;

wherein the agent includes a plurality of risk-assessment modules;

wherein the commands execute the risk-assessment modules in a specific manner that is configured at the remote computer;

wherein the commands each indicate at least one of the risk-assessment modules;

wherein the commands are processed by extracting parameters associated with the commands, and executing the risk-assessment modules indicated by the commands utilizing the associated parameters.

26. (Currently Amended) A computer program product embodied on a computer readable medium for remotely detecting vulnerabilities from a remote computer, comprising:
- a) computer code for sending encrypted commands from a remote computer to an agent on a local computer for executing a risk-assessment scan utilizing a network, the commands adapted for being decrypted and processed on the

-8-

local computer utilizing the agent for performing the risk-assessment scan on the local computer in accordance with the processed commands to remotely detect local vulnerabilities on the local computer;

b) computer code for receiving results of the risk-assessment scan from the local computer utilizing the network; and

c) computer code for transmitting feedback to the results from the remote computer to the local computer utilizing the network;

wherein the agent includes a plurality of risk-assessment modules;

wherein the commands execute the risk-assessment modules in a specific manner that is configured at the remote computer;

wherein the commands each indicate at least one of the risk-assessment modules;

wherein the commands are processed by extracting parameters associated with the commands, and executing the risk-assessment modules indicated by the commands utilizing the associated parameters.

27. (Currently Amended) A method of remotely detecting vulnerabilities on a local computer, comprising:

a) installing an agent on a local computer, the agent including a plurality of risk-assessment modules selected based on at least one aspect of the computer;

b) receiving encrypted commands for executing a risk-assessment scan from a remote computer utilizing a network;

c) decrypting the commands on the local computer utilizing the agent;

d) authenticating the commands on the local computer utilizing the agent;

e) processing the commands on the local computer utilizing the agent, the commands adapted to execute the risk-assessment modules in a specific manner that is configured at the remote computer;

f) performing the risk-assessment scan on the local computer in accordance with the processed commands to remotely detect local vulnerabilities on the local computer;

g) transmitting results of the risk-assessment scan from the local computer to the remote computer utilizing the network;

-9-

- h) receiving feedback to the results from the remote computer utilizing the network;
wherein the commands each indicate at least one of the risk-assessment modules;
wherein the commands are processed by extracting parameters associated with the commands, and executing the risk-assessment modules indicated by the commands utilizing the associated parameters.
28. (New) The computer program product as recited in claim 10, wherein the feedback is active.
29. (New) The computer program product as recited in claim 28, wherein the feedback includes additional commands and additional modules for correcting the vulnerabilities in response to the additional commands.
30. (New) The computer program product as recited in claim 10, wherein the feedback is passive.
31. (New) The computer program product as recited in claim 30, wherein the feedback includes descriptions as to how to correct the vulnerabilities.
32. (New) The computer program product as recited in claim 9, wherein the results include a log of the risk-assessment scan.
33. (New) The computer program product as recited in claim 32, wherein the results include an identification of the vulnerabilities.
34. (New) The computer program product as recited in claim 1, wherein a plurality of the commands are each associated with only one of the risk-assessment modules.

-10-

35. (New) The computer program product as recited in claim 1, wherein a different set of risk-assessment modules exists on different local computers, based on a platform associated with each of the local computers.